UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box.1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/667,582	09/22/2003	Jeffrey B. Parham	13768.604.17	9642

7590 11/17/2006

RICK D. NYDEGGER
WORKMAN NYDEGGER
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

EXAMINER	
SHAN, APRIL YING	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/667,582	PARHAM ET AL.	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 Septmber 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 Feburary 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/04/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 4-10 and 21-25 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

With respect to **claims 4-10**, a "controlling authority" is being recited; it appears that the system would reasonably be interpreted by one of ordinary skill in the art as software, per se. The controlling authority, an identity catalog, authority resolution module and network interface are all software disclosed in the Applicant's specification, for example, in par [0003], [0006] and [0021]. As such, it believes that the controlling authority of claims 4-10 are reasonably interpreted as functional descriptive material, per se.

With respect to **claims 21-25,** the "computer-readable medium," in accordance with Applicant's specification, includes data signal, such as a carrier wave on page 6-7 of the specification. This subject matter is not limited to that which falls within a statutory category of invention because it is not limited to a process, machine, manufacture, or a composition of matter. Instead, it includes a form of energy. Energy does not fall within a statutory category since it is clearly not a series of steps or acts to

constitute a process, not a mechanical device or combination of mechanical devices to constitute a machine, not a tangible physical article or object which is some form of matter to be a product and constitute a manufacture, and not a composition of two or more substances to constitute a composition of matter.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 4 and 6 are rejected under 35 U.S.C. 102(e) as being anticipated by Crane et al. (U.S. Patent No. 6,510,236).

As per **claim 4**, Crane et al. discloses a controlling authority (application server 12 in fig. 1 corresponds to Applicant's a controlling authority) for identifying an authenticating authority (application authentication server 17 in fig. 4 corresponds to Applicant's authentication authority) for authenticating a principal for access to network resources comprising:

an identity catalog ("a local database 15 or a network directory service" – e.g. col. 5, lines 3-4) mapping at least one account ID ("Typically, an authentication device or

device type is supported if there is a device authentication server 18 available to the framework. A given device authentication 18 typically registers with the application server for this purpose" – e.g. col. 3, lines 54-58 and col. 3, lines 13-16) of at least one principal to an identifier of a corresponding authenticating authority ("The particular device authentication server selected by the application server depends on the authentication device or its type" – e.g. col. 5, lines 18-20); and

an authority resolution module ("The invention framework preferably is implemented in software residing on the client, the application server, and the individual authentication device servers..." – e.g. col. 6, lines 25-36) for accessing the identity catalog to match the account ID with a corresponding authenticating authority (e.g. col. 5, lines 1-8) and for causing an authentication request to be directed to the corresponding authenticating authority ("...and then forwards authentication data in the request to that server" – e.g. abstract. Please note that server is the corresponding authenticating authority).

As per **claim 6**, Crane et al. discloses the controlling authority as claimed in claim 4. Crane et al. further discloses wherein the identity catalog maps a plurality of account IDs to a corresponding plurality of authenticating authorities ("...In particular, each authentication device may be registered with the framework, in which case a complete list of authentication devices is provided in the database 15" – e.g. col. 5, lines 6-8 and "Each device type typically has its own authentication device server 18. Thus,

the framework has multiple authentication device servers 18 associated therewith" – e.g. col. 3, lines 14-16).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 1-3, 11-13, 15-19 and 21-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Martherus et al. (US Pub No. 2002/0112155) in view of Crane et al. (U.S. Patent No. 6,510,236).

As per **claim 1**, Martherus et al. discloses a method of authenticating a principal in a network environment for access to secured resources ("...capable of authentication a user for a plurality of domains in a network-based system..." – e.g. paragraph [0011]) comprising:

receiving at an authority (Web server 18 in fig. 1 corresponds to Applicant's an authority) a login request from the principal, wherein the login request comprises an account identifier ("Fig. 32 provides an exemplar method for performing...authentication...In response, the user enters and the user's browser submits the requested user ID and password...In step 1206, Web Gate 28 intercepts the user submission.. – e.g. paragraph [0204] and fig. 32);

transmitting the account identifier from the receiving authority to a super authority to authenticate the principal ("...passes the user ID and password to Access Server..." - e.g. paragraph [0204] and step 1206 in fig. 32); and

authenticating the principal at the super authority ("Access Server authentication module 540 then authenticates the user using the user ID and password in step 1208. In step 1210, authentication module 540 returns the authentication result..." – e.g. paragraph [0204] and steps 1208, 1210 in fig. 32).

Martherus et al. discloses receiving the authentication requests, transmitting the request to the super authority and authenticating the principal at super authority. But it

fails to disclose the limitations for using super authority to direct authentication requests to the appropriate authorities and the appropriate authorities will authenticate principals.

However, such missing limitations in Martherus et al. is clearly taught in the aforementioned Crane et al. reference by disclosing ("The invention accomplished this object by using the application server as a "traffic cop" or router to manage authentication requests from the various clients" in col. 3, lines 38-41, "...The application server, however, does not perform an authentication function with respect to the data. Rather, it first determines whether the authentication device or device type...This evaluation is typically effected by scanning a local database...The particular device authentication server selected by the application server depends on the authentication device or its type" in col. 4, lines 64 – col. 5, line 20. Please note "application server 12" in fig. 1 corresponds to Applicant's super authority and "authentication server 18" in fig. 1 corresponds to Applicant's authority)

Martherus et al. and Crane et al. are analogous art in that they are of the same field of endeavor, that is, a system and/or method of an authentication framework for authenticating clients. It would have been obvious to a person of ordinary skill in the art at the time of the invention to incorporate such well known feature as taught in the Crane et al. reference into the Martherus et al. system motivated by "to provide an authentication architecture that enables client-server and Internet based applications to use alternate authentication devices, e.g., token cards and biometric devices and to provide an application server with the capability of managing authentication request traffic from a variety of clients having disparate authentication devices or schemes. And

...in addition, because authentication data is stored on separate authentication device servers, security is enhanced" (col. 1, line 61 – col. 2, line 4 and col. 5, line 65 – col. 6, line 24), as taught by Crane et al.

As per **claim 2**, the combined teachings of Martherus et al. and Crane et al. disclose the method as applied in claim 1. Martheurs et al. further discloses wherein the account identifier comprises a principal identifier and a namespace identifier ("The user enters and the user's browser submits the requested user ID and password." – e.g. paragraph [0204]).

As per **claim 3**, the combined teachings of Martherus et al. and Crane et al. disclose the method as applied in claim 1. Martheurs et al. further discloses receiving at the receiving authority from the super authority a request to authenticate a second principal based on a login request made by the second principal, wherein the login request made by the second principal was made by the requesting principal to another authority other than the receiving authority ("user access requests for a protected resource in a first domain are received and redirected to a second domain. User authentication is performed at the second domain" – e.g. abstract).

As per **claims 11 and 17**, Martherus et al. discloses a method/apparatus of controlling authentication of principals for access to network resources in a network environment comprising:

Receiving a request for an authenticating authority resolution from one of a plurality of authenticating authorities (Web server 18 in fig. 1 corresponds to Applicant's an authority), wherein the request comprises an account ID of a principal to be authenticated ("Fig. 32 provides an exemplar method for performing...authentication...In response, the user enters and the user's browser submits the requested user ID and password...In step 1206, Web Gate 28 intercepts the user submission.. – e.g. paragraph [0204] and fig. 32);

But Martherus et al. fails to disclose the limitations for using super authority to direct authentication requests to the appropriate authorities and the appropriate authorities will authenticate principals

However, such missing limitations in Martherus et al. is clearly taught in the aforementioned Crane et al. reference by disclosing ("The invention accomplished this object by using the application server as a "traffic cop" or router to manage authentication requests from the various clients" in col. 3, lines 38-41, "...The application server, however, does not perform an authentication function with respect to the data. Rather, it first determines whether the authentication device or device type...This evaluation is typically effected by scanning a local database...The particular device authentication server selected by the application server depends on the authentication device or its type" in col. 4, lines 64 – col. 5, line 20. Please note "application server 12 in fig. 1 corresponds to Applicant's super authority and "authentication server 18 in fig. 1 corresponds to Applicant's authority).

Martherus et al. and Crane et al. are analogous art in that they are of the same field of endeavor, that is, a system and/or method of an authentication framework for authenticating clients. It would have been obvious to a person of ordinary skill in the art at the time of the invention to incorporate such well known feature as taught in the Crane et al. reference into the Martherus et al. system motivated by "to provide an authentication architecture that enables client-server and Internet based applications to use alternate authentication devices, e.g., token cards and biometric devices and to provide an application server with the capability of managing authentication request traffic from a variety of clients having disparate authentication devices or schemes. And ...in addition, because authentication data is stored on separate authentication device servers, security is enhanced" (col. 1, line 61 – col. 2, line 4 and col. 5, line 65 – col. 6, line 24), as taught by Crane et al.

As per claims **12-13 and 18-19**, the combined teachings of Martherus et al. and Crane et al. disclose the method/apparatus as applied in claims 11 and 17. Crane et al. further discloses wherein each account ID comprises a namespace identifier ("user (id) as well as device (id)" – e.g. col. 4, lines 58-63). And in col. 5, lines 45-50, Crane et al. additionally discloses "A plurality of device authentication servers are supported by the framework, preferably with at least one server providing authentication services for each type of authentication device supported. This allows any supported device authentication server to verify data from any supported authentication device on the network". Therefore, it would have been obvious for a person having ordinary skill in

the art at the time of the invention that the plurality of account IDs comprises at least two account IDs having a common namespace identifier (two different user ID with same device type/id) can be mapped to at least two different respective ones of the plurality of authenticating authorities and/or that the plurality of account IDs comprises at least two account IDs having different namespace identifiers (two different user ID with different device type/id) can be mapped to the same one of the plurality of authenticating authorities. The motivation of doing so, "to allow any supported device authentication server to verify data from any supported authentication device on the network", as taught in col. 5, lines 48-50 and to balance workload of each authentication server.

As per **claim 15**, the combined teachings of Martherus et al. and Crane et al. disclose the method as applied in claims 11. Martherus et al. further discloses wherein the assignment mapping is based at least in part on the organizational affiliation of principals within an entity (fig. 4 and paragraphs [0100]-[0102]).

As per **claim 16**, the combined teachings of Martherus et al. and Crane et al. disclose the method as applied in claims 11. Martherus et al. further discloses wherein the assignment mapping is based at least in part on the geographical location of principals (fig. 4).

As per **claims 21-25**, the combined teachings of Martherus et al. and Crane et al. disclose the claimed method of steps as applied above in claims 11-13 and 15-16. Therefore, the combined teachings of Martherus et al. and Crane et al. disclose the claimed computer-executable instructions embodied in a computer-readable medium for carrying out the method of steps.

10. Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crane et al.

As per **claims 7-8**, Crane et al. discloses a controlling authority as applied in claim 6. Crane et al. further discloses wherein each account ID comprises a namespace identifier ("user (id) as well as device (id)" – e.g. col. 4, lines 58-63). And in col. 5, lines 45-50, Crane et al. additionally discloses "A plurality of device authentication servers are supported by the framework, preferably with at least one server providing authentication services for each type of authentication device supported. This allows any supported device authentication server to verify data from any supported authentication device on the network". Therefore, it would have been obvious for a person having ordinary skill in the art at the time of the invention that the plurality of account IDs comprises at least two account IDs having a common namespace identifier (two different user ID with same device type/id) can be mapped to at least two different respective ones of the plurality of authenticating authorities and that the plurality of account IDs comprises at least two account IDs having different namespace identifiers (two different user ID with different device type/id) can be

mapped to the same one of the plurality of authenticating authorities. The motivation of doing so, "to allow any supported device authentication server to verify data from any supported authentication device on the network", as taught in col. 5, lines 48-50 and to balance workload of each authentication server.

11. Claims 5, 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crane et al. as applied to claims 4-6 above, and further in view of Martherus et al. (U.S. Pub No. 2002/0112155).

As per **claim 5**, Crane et al. discloses a controlling authority as applied in claim 4. Crane et al. is silent on a network interface for passing the account ID to the authority resolution module and for receiving from the authority resolution module an authentication request directed to the corresponding authenticating authority. However, such missing feature in Crane et al. is clearly taught in the paragraph [0083] "Web Gate 28 acts as an interface between Web Server 18 and Access Server 34. Web Gate 28 intercepts requests from users for resources, and authorizes them via Access Server 34 and paragraph [0194]" of the aforementioned Martherus et al. reference, the same field endeavor. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Martherus et al. reference into Crane et al.'s controlling authority motivated by to provide "an interface between Web Server and Access server and to redirect user authentication exchanges to the e-business host's designated web log-in Web Server", as taught in paragraph [0083] and [0194] of the Martherus et al. reference.

As per **claim 9**, Crane et al. discloses a controlling authority as applied in claims 4 and 6 above. Crane et al. is silent on the content of the identity catalog is based at least in part on the organizational affiliation of principals within an entity. However, such missing feature in Crane et al. is clearly taught in the fig. 4 and paragraphs [0100]-[0102] of the aforementioned Martherus et al. reference, the same field endeavor. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Martherus et al. reference into Crane et al.'s controlling authority motivated by "to help manage the users", as taught in paragraph [0100] of the Martherus et al. reference.

As per **claim 10**, Crane et al. discloses a controlling authority as applied in claims 4 and 6 above. Crane et al. is silent on the content of the identity catalog is based at least in part on the geographical location of principals. However, such missing feature in Crane et al. is clearly taught in the fig. 4 of the aforementioned Martherus et al. reference, the same field endeavor. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Martherus et al. reference into Crane et al. controlling authority motivated by "to help manage the users", as taught in paragraph [0100] of the Martherus et al. reference.

12. Claims 14 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Martherus et al. (US Pub No. 2002/0112155) and Crane et al. (U.S. Patent No.

6,510,236) as applied to claims 11-13 above, further in view of Hacherl (U.S. Patent No. 6,324,571)

As per claims **14 and 20**, the combined teachings of Martherus et al. and Crane et al. disclose the method/apparatus as applied in claims 11 and 17.

The combined teachings fail to disclose altering the assignment mapping whereby an account ID previously mapped to a first authenticating authority is remapped to a second authenticating authority. However, such missing limitations in the combined teachings in Martherus et al. and Crane et al. is taught in the aforementioned Hacherl reference by disclosing switching exclusive authority (corresponds to Applicant's authorized authentication authority) to perform a predefined system-wide task (e.g. authenticate a particular principal) in a network environment. (see abstract of Hacherl)

Martherus et al., Crane et al. and Hacherl are analogous art in that they are of the same field of endeavor, that is, method/apparatus of performing system-wide tasks in a network environment. It would have been obvious to a person of ordinary skill in the art at the time of the invention to incorporate such well known feature as taught in the Hacherl reference into the combined teachings of Martherus et al. and Crane et al.'s method/apparatus motivated by "Exclusive authority to perform the task should be easily transferred between machines, however, so as to avoid the limitations of prior single server design", as taught by Hacherl (col. 1, lines 61-64)

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Scott et al. (U.S. Pub. No. 2003/0233328) discloses in a computer network, comprising a plurality of authentication servers connected to the communications network, an authentication server selector selects that determines a near authentication server for the user computer from the plurality of authentication servers.
- Guo et al. (U.S. Pub. No. 2002/0143964) discloses a computerized method and system for routing between network servers.
- Guo et al. (U.S. Patent No. 6,912,582) discloses a computerized method and system for routing between network servers.
- Schmidt et al. (U.S. Pub. No. 2003/0120948) discloses an enterprise network architecture has trust link established between two autonomous network systems that enables transitive resource access between network domains of the two network systems.
- Kobata et al. (U.S. Pub. No. 2006/0005237) discloses technique for using an authentication proxy server for a destination server to authenticate the identity of the user.
- Peles (U.S. Pub. No. 2004/0177247) discloses when a user makes a request to a server for a specific service, a decision must be made as to whether the user's

traffic should be forwarded to the server providing the requested service and where to forward the user's traffic.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

6 November 2006
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100